NOMBRE DEL CURSO

Diplomado en Ciberseguridad

TIPO DE INSTANCIA

Diplomado

SEDE DE ORIGEN

Sede Mendoza

DURACIÓN

120 horas reloj.

PRESENTACIÓN/FUNDAMENTACIÓN DE LA PROPUESTA

En el actual escenario de transformación digital, las organizaciones de la región, y en particular en sectores productivos de Mendoza, enfrentan una sofisticación sin precedentes en las amenazas cibernéticas. La transición hacia la Industria 4.0 ha borrado la frontera entre el mundo físico (OT) y el digital (IT), exponiendo activos críticos a riesgos que pueden comprometer la continuidad de las operaciones.

Este diplomado surge para cubrir la brecha de talento técnico capaz de diseñar y gestionar estrategias de defensa robustas. A diferencia de ofertas puramente teóricas, esta propuesta utiliza un caso práctico transversal, con la situación inicial de una PyME industrial local que evoluciona a lo largo del cursado, permitiendo a los estudiantes aplicar herramientas *Open-Source* y metodologías corporativas (NIST, MITRE ATT&CK) en un entorno controlado pero de alta fidelidad.

OBJETIVO GENERAL

Formar profesionales con competencias teóricas y prácticas en ciberseguridad, capacitándolos para identificar, analizar, prevenir y responder a amenazas digitales mediante la implementación de soluciones de protección en infraestructuras de red, sistemas y aplicaciones.

OBJETIVOS ESPECÍFICOS

- Identificar y mitigar amenazas modernas y vectores de ataque comunes en entornos corporativos

e industriales.

- Diseñar e implementar arquitecturas de seguridad perimetral y segmentación de redes utilizando herramientas de código abierto.
- Gestionar el control de acceso y la identidad bajo el modelo de "Confianza Cero" (Zero Trust).
- Analizar el impacto y las aplicaciones de la Inteligencia Artificial tanto en la ejecución de ataques como en la automatización de la defensa.
- Desarrollar planes de respuesta ante incidentes (IRP) y ejecutar análisis forense básico tras una brecha de seguridad.

DESTINATARIOS/AS

La propuesta está orientada a:

- Profesionales de IT, administradores de red y desarrolladores de software.
- Responsables de infraestructura tecnológica.
- Técnicos egresados de carreras afines que busquen especialización en seguridad informática.
- Emprendedores tecnológicos que necesiten asegurar sus activos digitales.

REQUISITOS

Conocimientos básicos de redes (protocolo TCP/IP) y sistemas operativos (Windows/Linux).

MODALIDAD / METODOLOGÍA

Se adopta un enfoque pedagógico de "Aprender haciendo" (Learning by doing):

- **Clases sincrónicas:** Exposición de conceptos y debates interactivos.
- **Laboratorios Prácticos:** Uso de contenedores Docker-Compose que simulan redes corporativas reales para prácticas de ataque y defensa.
- **Aula Virtual:** Repositorio de materiales, foros de discusión y entrega de asignaciones.

Se prevé una distribución horaria de **50 horas de participación sincrónica** (encuentros virtuales en vivo) y de **70 horas de actividad asincrónica** (trabajo en plataforma, laboratorios y lecturas).

CRITERIOS DE EVALUACIÓN Y CERTIFICACIÓN

Para la obtención de la certificación del ITU-UNCUYO, el/la estudiante deberá cumplir con:

- **Asistencia:** Mínimo del 75% a las clases sincrónicas.
- **Participación:** Cumplimentar las actividades propuestas en los foros del aula virtual (20% de la nota).
- **Laboratorios:** Aprobación de los 5 laboratorios prácticos (40% de la nota).
- **Proyecto Integrador:** Defensa y aprobación del proyecto final (40% de la nota).

Calificación mínima para aprobación: 6 (seis) sobre 10 (diez).

CONTENIDOS

Módulo 1: Fundamentos y Superficie de Ataque

- Introducción a la Ciberseguridad: Triada CID y normativas (Ley 25.326 y 26.388).
- Anatomía de un ataque: El ciclo de vida del exploit.
- Modelado de amenazas. Caso práctico.
- *Laboratorio 1:* Reconocimiento y escaneo de vulnerabilidades con herramientas Open-Source.

Módulo 2: Seguridad Perimetral y Redes

- Defensa en profundidad: Firewalls, IPS/IDS y segmentación de red.
- Protocolos seguros y endurecimiento (Hardening) de sistemas operativos.
- *Laboratorio 2:* Implementación de reglas de filtrado y detección de intrusos.

Módulo 3: Identidad, Acceso y Terminales (Endpoints)

- Gestión de Identidad y Acceso (IAM): Autenticación multifactor (MFA).
- Seguridad en el Endpoint: Del Antivirus tradicional al EDR/XDR.
- *Laboratorio 3:* Simulación de protección contra Ransomware en estaciones de trabajo.

Módulo 4: Ciberseguridad e Inteligencia Artificial

- IA Generativa: Uso de LLMs para la creación de código defensivo y detección de anomalías.
- Amenazas potenciadas por IA: Phishing automatizado y Deepfakes.
- *Laboratorio 4:* Automatización de alertas de seguridad mediante scripts potenciados por IA.

Módulo 5: Operaciones de Seguridad y Respuesta a Incidentes

- Monitoreo y SOC (Security Operations Center).
- Plan de Respuesta a Incidentes (IRP) y recuperación ante desastres (DRP).
- *Laboratorio 5:* Mitigación de un ataque activo en tiempo real sobre la infraestructura. Caso práctico.

Proyecto Integrador Final

- Aplicación transversal de los 5 módulos para el diseño de una estrategia de seguridad integral para un caso de uso real o simulado.